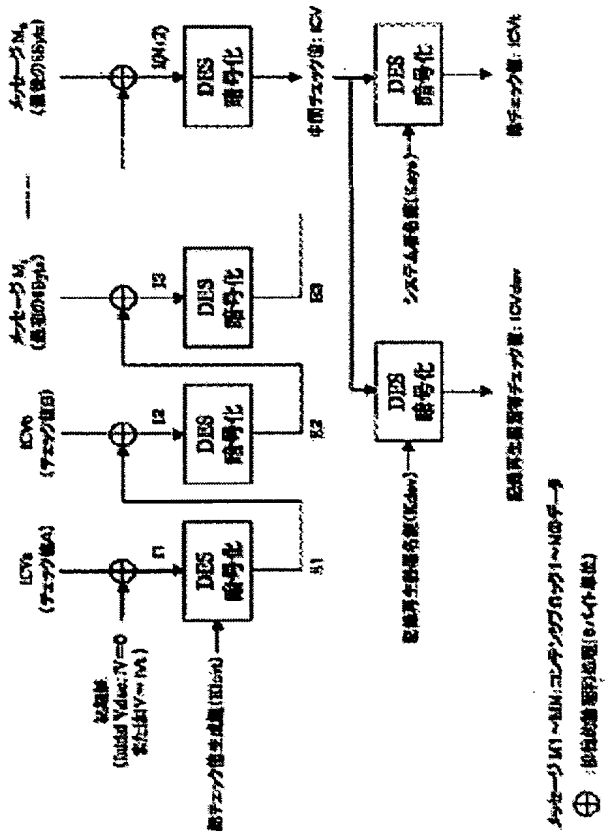
DEVICE AND METHOD FOR DATA PROCESSING AND PROGRAM PROVIDING MEDIUM

Publication number: JP2001211149
Publication date: 2001-08-03
Inventor: ISHIBASHI YOSHITO; ASANO TOMOYUKI; AKISHITA TORU; SHIRAI TAIZO
Applicant: SONY CORP
Classification:
- international: ***G09C1/00; G11B20/10; H04L9/08;*** **G09C1/00; G11B20/10; H04L9/08;** (IPC1-7): H04L9/08; G09C1/00; G11B20/10
- European:
Application number: JP20000016029 20000125
Priority number(s): JP20000016029 20000125

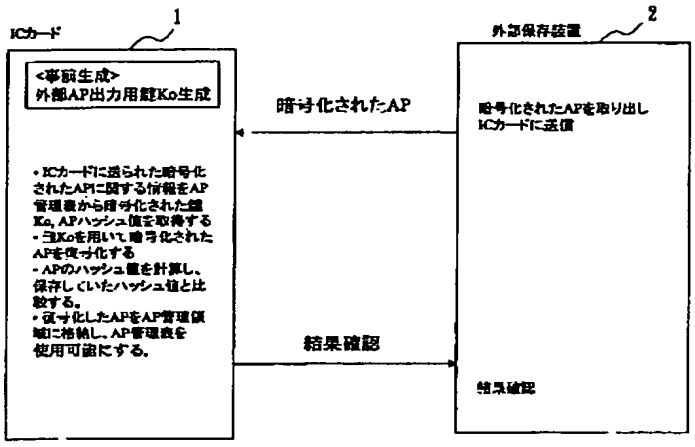
Report a data error here

Abstract of **JP2001211149**

PROBLEM TO BE SOLVED: To provide a data processor which can reproduce contents only when specified according to the use limitation of the contents. SOLUTION: A device unique key characteristic of a data professor such as a receding and reproducing device and a PC using content data and a system common key which is common to other data processors using the contents data are stored. The data processor selectively uses those keys for the contents according to the use limitation of the contents. For example, the data processor uses the key characteristic of itself for contents which are usable only by the data processor and the common key for contents that even other systems can use to generate a check value of the contents and perform a matching process, and deciphers and reproduces the ciphered data only when the marching process is successful.



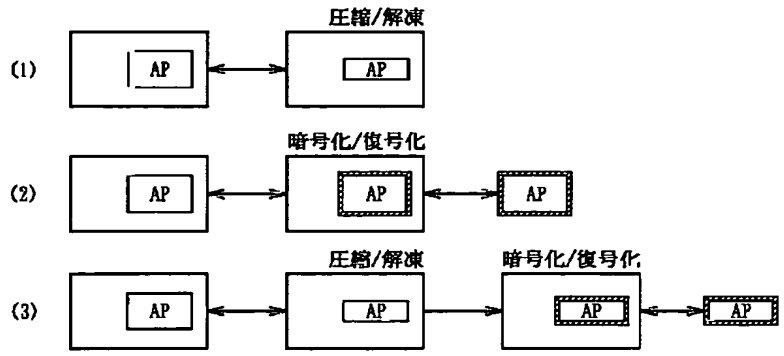
【図4】



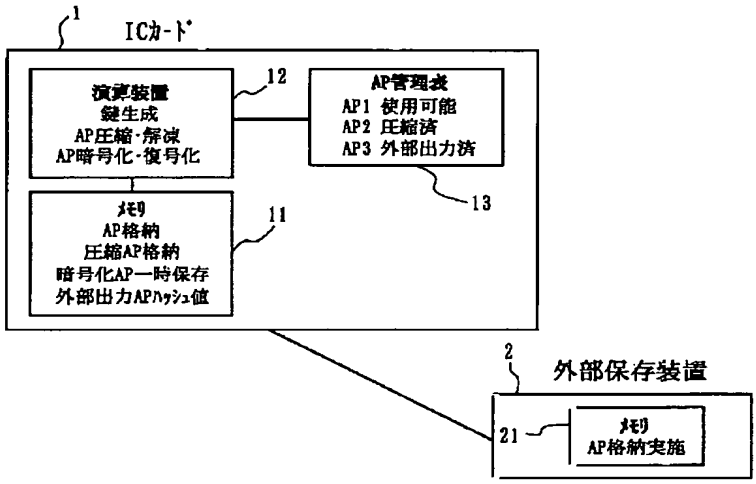
フロントページの続き

Fターム(参考) 2C005 MA40 MB03 SA21
5B035 BB09 CA29
5B058 CA23 KA08 YA20
5B076 FA00

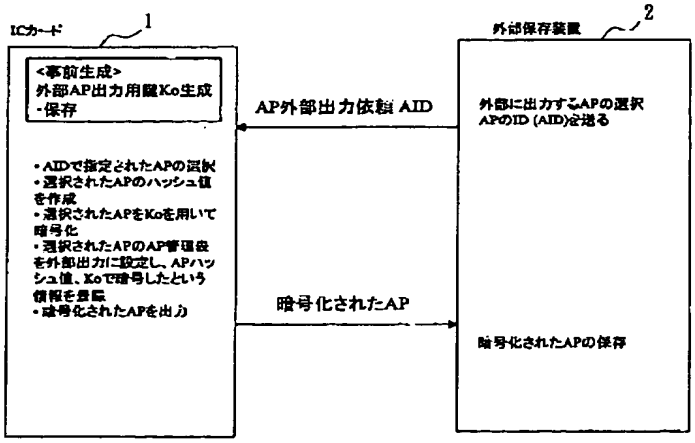
【図１】


圧縮/解凍
(1)
AP
AP
暗号化/復号化
(2)
AP
AP
AP
圧縮/解凍
暗号化/復号化
(3)
AP
AP
AP
AP

【図２】


1
ICカード
演算装置
鍵生成
AP圧縮・解凍
AP暗号化・復号化
12
AP管理表
AP1 使用可能
AP2 圧縮済
AP3 外部出力済
13
メモリ
AP格納
圧縮AP格納
暗号化AP一時保存
外部出力APハッシュ値
11
2
外部保存装置
21
メモリ
AP格納実施

【図３】


ICカード
1
<事前生成>
外部AP出力用鍵Ko生成
・保存
・AIDで指定されたAPの選択
・選択されたAPのハッシュ値を作成
・選択されたAPをKoを用いて暗号化
・選択されたAPのAP管理表を外部出力に設定し、APハッシュ値、Koで暗号したという情報を登録
・暗号化されたAPを出力
AP外部出力依頼 AID
暗号化されたAP
外部保存装置
2
外部に出力するAPの選択
APのID (AID)を送る
暗号化されたAPの保存

参照して説明する。図2は本発明方法を実施する装置の構成図を示し、図3及び図4は本発明の方法においてアプリケーションを暗号化して出力する手順及び復号化して再格納する手順を示す。ＩＣカード１には複数のアプリケーションＡＰ１、ＡＰ２、ＡＰ３がメモリ１１に格納され、各アプリケーションの状態がアプリケーション管理テーブル１３で管理されている。例えば、図2の例ではアプリケーションＡＰ１は使用可能（圧縮も外部に出力もされてない）、ＡＰ２は圧縮済(使用不可)、ＡＰ３は外部出力済(使用不可)である。ＩＣカード１には、暗号化復号化のための鍵Koがカード内の演算装置１２で事前に生成され、保存されている。

【００１１】ＩＣカード１の使用可能カード容量を増やしたいときには、利用者は暫く不要なアプリケーションをパソコンのような外部保存装置２で選択し、選択したアプリケーションのＩＤ（ＡＩＤ）をＩＣカード１にアプリケーション外部出力依頼とともに送信する(図3)。ＩＣカード１はＡＩＤで指定されたアプリケーションを選択し、演算装置１２で選択されたアプリケーションのハッシュ値を計算し、選択されたアプリケーションを事前に保存した鍵Koを用いて暗号化し、アプリケーション管理表１３内の選択されたアプリケーションの状態を「外部出力」に設定するとともに、このアプリケーションのハッシュ値、鍵Koで暗号化したという情報を登録した後、暗号化されたアプリケーションを外部保存装置２へ送信し、外部保存装置２はこれをメモリ２１に保存する。

【００１２】外部保存装置２に保存した暗号化されたアプリケーションが必要になったときには、利用者はこの暗号化されたアプリケーションを外部保存装置２のメモリ２１から読み出し、ＩＣカード１へ送信する(図4)。ＩＣカード１は送られてきた暗号化されたアプリケーションに関する情報、即ち鍵Ko、アプリケーションハッシュ値をアプリケーション管理表１３をから取り出し、鍵Koを用いて暗号化されたアプリケーションを復号化し、復号化されたアプリケーションのハッシュ値を計算し、保存していたハッシュ値と比較し、一致する場合に、復号化されたアプリケーションをメモリ１１のアプリケーション格納部に格納するとともに、アプリケーション管理表１３内のこのアプリケーションの状態を 外部出力 から「使用可能」にする。最後に、再格納の結果を外部保存装置２に通知し、処理を終了する。

【００１３】上述の実施例では、暫く不要なアプリケーションを暗号化して外部に出力する際、ＩＣカード内で生成させた鍵Koで暗号化したものを出力させるが、
①アプリケーションをＩＣカードに格納されているカード発行者のデータ保存用の鍵K_{CI}で暗号化したものを出力させる、
②アプリケーションを鍵Koで暗号化したものとアプリケーションをカード発行者の鍵で暗号化されたものの両方を出力させる、又は
③鍵Koで暗号化したものと鍵Koをカード発行者の鍵で暗号化したものを出力させることができる。

【００１４】①～③には、カード発行者がカード外に出されたアプリケーションを復号化して、内容を解析、確認することができるので、利用者が勝手なアプリケーションを格納するのをチェックすることができる。 ②、③の場合には、利用者とカード発行者の両方がカード外に出されたアプリケーションを保存するので、利用者が外部保存したアプリケーションを消去又は紛失してしまった場合にもこれをバックアップすることができる。以上、本発明を複数のアプリケーションが格納されたＩＣカードについて詳細に説明したが、本発明は複数のアプリケーションが格納された携帯端末にも同様に適用し得ること勿論である。

【００１５】

【発明の効果】本発明によれば、ＩＣカード内にあるアプリケーションのうちいくつか又は全てを圧縮することにより、又は暗号化して一度外部に安全に保存することにより、カード容量が増えるので、カード容量が増えた分、他のアプリケーションをＩＣカードに入れて使用することが可能になる。また、圧縮又は一度外部に保存したアプリケーションについても、カード内に再格納することにより、再び安全に使用することが可能になる。

【図面の簡単な説明】

【図１】 本発明によるアプリケーション格納ＩＣカードの使用可能カード容量増大方法の手順の概要を示す図である。

【図２】 本発明の方法を実施する装置の構成図である。

【図３】 本発明の方法においてアプリケーションを暗号化して出力する手順を示す図である。及び復号化して再格納する手順を示す。

【図４】 本発明の方法において外部に出力された暗号化アプリケーションを復号化して再格納する手順を示す図である。

【符号の説明】

１ ＩＣカード
１１ メモリ
１２ 演算装置
１３ アプリケーション管理表
２ 外部保存装置
２１ メモリ

ーションを格納し、複数のサービスを提供するマルチアプリケーションＩＣカードや、種々のデータを格納するデータ格納カードが広く使われている。また、携帯電話の発展に伴い、最近では複数のアプリケーションをメモリに格納して複数のサービスを受けることができる携帯端末が出現している。

【０００３】

【発明が解決しようとする課題】従来、ＩＣカードのような耐タンパ装置や携帯端末に一度アプリケーション又はデータを格納すると、使用可能記憶容量を増やすためには、格納したアプリケーション又はデータの一部又は全部を一旦削除する他に方法がなかった。そのため、ＩＣカード又は携帯端末にないアプリケーション又はデータをＩＣカード又は携帯端末に格納するためには、必要なアプリケーション又はデータであっても削除するしかなかった。本発明の目的は、安全に且つＩＣカードのような耐タンパ装置や携帯端末内のアプリケーション又はデータを削除する必要なしカード容量を増やす方法及び装置を提供することにある。

【０００４】

【課題を解決するための手段】本発明では、ＩＣカードや携帯端末等のようなアプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量を増やすために、当該装置の少なくとも１つのアプリケーション又はデータを、(1)当該装置内にて圧縮する、(2)当該装置内にて暗号化して外部に出力し保存する、又は(3)当該装置内にて圧縮した後に暗号化して外部に出力し保存する、ことを特徴とする。

【０００５】本発明では、更に、(1)圧縮したアプリケーション又はデータが必要になった際にはこれを解凍し、使用可能とする、(2)外部に保存した暗号化されたアプリケーション又はデータが必要になった際にはこれを当該装置に戻し、当該装置内にて復号化してメモリに再格納する、(3)外部に保存した暗号化された圧縮アプリケーション又はデータが必要になった際にはこれを当該装置に戻し、当該装置内にて復号化し、解凍してメモリに再格納する、ことを特徴とする。

【０００６】本発明では、ＩＣカードや携帯端末等のようなアプリケーション又はデータ格納メモリを具えた装置において、少なくとも１つのアプリケーション又はデータが格納されたメモリの使用可能記憶容量を増やすために、前記メモリ内の選択されたアプリケーション又はデータを圧縮し、再使用に解凍する機能、暗号化して外部に出力し、再格納時に復号化する機能、圧縮した後暗号化して外部に出力し、再格納時に復号化した後解凍する機能を有する演算装置と、前記メモリ内に格納されているアプリケーション又はデータの状態が使用可能か、圧縮中か、外部出力中かを示すアプリケーション又はデータ管理表と、を設けたことを特徴とする。

【０００７】

【発明の実施の形態】本発明を図面を参照して以下に詳細に説明する。図１は本発明によるアプリケーション格納ＩＣカードの使用可能カード容量増大方法の手順の概要を示す。本発明では、アプリケーション格納ＩＣカードの使用可能カード容量を増やすために、

(1)ＩＣカード内の暫く不要なアプリケーションＡＰを圧縮する。圧縮したアプリケーションが必要になった際にはこれを解凍し、使用可能にする。

(2)ＩＣカード内にて暫く不要なアプリケーションを圧縮せずに暗号化して外部に出力し、所望の外部保存装置に保存する。外部に保存した暗号化されたアプリケーションが必要になった際にはこれをＩＣカードに戻し、復号化して使用可能にする。

(3)ＩＣカード内にて暫く不要なアプリケーションＡＰを圧縮し、圧縮したアプリケーションを暗号化して外部に出力し、所望の外部保存装置に保存する。外部に保存した暗号化された圧縮アプリケーションが必要になった際にはこれをＩＣカードに戻し、復号化し、解凍して使用可能にする。

【０００８】第２及び第３の方法によれば、暫く不要なアプリケーションをＩＣカードの外へ出すので、第１の方法よりカード容量が増えるが、外に出したアプリケーションをＩＣカードに再格納する際には、そのアプリケーションが確かにこのカードに格納されていたものか確認する必要がある。このため、第２の方法では、ＩＣカード内にて暗号化・復号化のための鍵を生成し、しばらく不要なアプリケーションのハッシュ値を取り、メモリ等に保存し、そのアプリケーションを先に生成した鍵により暗号化し、ＩＣカードの外部に出力する。外部に出力したアプリケーションをＩＣカードに再格納する際には、これを先に生成した鍵により復号化し、復号化されたアプリケーションのハッシュ値を計算し、先に保存していたハッシュ値と比較し、一致する場合にのみ、復号化されたアプリケーションをカードに格納する。

【０００９】第３の方法では、ＩＣカード内にて暗号化・復号化のための鍵を生成し、しばらく不要なアプリケーションを圧縮し、圧縮したアプリケーションのハッシュ値を取り、メモリ等に保存し、圧縮したアプリケーションを先に生成した鍵により暗号化し、ＩＣカードの外部に出力する。外部に出力したアプリケーションをＩＣカードに再格納する際には、これを先に生成した鍵により復号化し、復号化された圧縮アプリケーションのハッシュ値を計算し、先に保存していたハッシュ値と比較し、一致する場合にのみ、復号化された圧縮アプリケーションを解凍してをカードに格納する。第３の方法では、アプリケーションを圧縮してから暗号化するので、暗号化のために必要とされるＩＣカード内の暗号化スペースが小さくなる。

【００１０】

【実施例】次に、本発明方法の一実施例を図２～図４を

【特許請求の範囲】
【請求項１】　ＩＣカードや携帯端末等のようなアプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量を増やすために、当該装置内の少なくとも１つのアプリケーション又はデータを、(1)当該装置内にて圧縮する、(2)当該装置内にて暗号化して外部に出力し保存する、又は(3)当該装置内にて圧縮した後に暗号化して外部に出力し保存する、ことを特徴とするアプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量増大方法。
【請求項２】　請求項１記載の方法において、(1)圧縮したアプリケーション又はデータが必要になった際にはこれを解凍し、使用可能とする、(2)外部に保存した暗号化されたアプリケーション又はデータが必要になった際にはこれを当該装置に戻し、当該装置内にて復号化してメモリに再格納する、(3)外部に保存した暗号化された圧縮アプリケーション又はデータが必要になった際にはこれを当該装置に戻し、当該装置内にて復号化し、解凍してメモリに再格納する、ことを特徴とするアプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量増大方法。
【請求項３】　請求項２記載の方法において、当該装置内にて暗号化・復号化のための鍵を予め生成し、前記(2)においてアプリケーション又はデータを暗号化して出力し、復号化して再格納する際に、アプリケーション又はデータのハッシュ値を取り、メモリ等に保存し、そのアプリケーション又はデータを予め生成した鍵により暗号化し、外部に保存し、外部に保存したアプリケーション又はデータを当該装置に再格納する際には、これを予め生成した鍵により復号化し、復号化されたアプリケーション又はデータのハッシュ値を計算し、先に保存していたハッシュ値と比較し、一致する場合にのみ、復号化されたアプリケーション又はデータを当該装置に格納すること、上記(3)においてアプリケーション又はデータを圧縮した後暗号化して出力し、復号化したのち解凍して再格納する際に、アプリケーション又はデータを圧縮し、圧縮したアプリケーション又はデータのハッシュ値を取り、メモリ等に保存し、圧縮したアプリケーション又はデータを予め生成した鍵により暗号化し、外部に保存し、外部に保存したアプリケーション又はデータを当該装置に再格納する際には、これを予め生成した鍵により復号化し、復号化されたを圧縮アプリケーション又はデータのハッシュ値を計算し、先に保存していたハッシュ値と比較し、一致する場合にのみ、復号化された圧縮アプリケーション又はデータを解凍して当該装置に格納することを特徴とするアプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量増大方法。
【請求項４】　請求項２又は３記載の方法において、上記(1)におけるアプリケーション又はデータの圧縮時に、アプリケーション又はデータ管理表内の対応するアプリケーション又はデータの状態を圧縮中にし、解凍時に使用可能にし、前記(2),(3)におけるアプリケーション又はデータの外部出力時に、アプリケーション又はデータ管理表内の対応するアプリケーション又はデータの状態を外部出力中にし、再格納時に使用可能にすることを特徴とするアプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量増大方法。
【請求項５】　請求項３記載の方法において、前記暗号化・復号化のための鍵の代わりに当該装置内に予め格納されている当該装置発行者の鍵を用いることを特徴とするアプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量増大方法。
【請求項６】　請求項３記載の方法において、前記暗号化・復号化のための鍵で暗号化されたアプリケーション又はデータとともに、当該装置内に予め格納されている当該装置発行者の鍵で暗号化されたアプリケーション又はデータも外部に出力することを特徴とするアプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量増大方法。
【請求項７】　請求項３記載の方法において、前記暗号化・復号化のための鍵で暗号化されたアプリケーション又はデータとともに、前記暗号化・復号化のための鍵を当該装置に予め格納されている当該装置発行者の鍵で暗号化したものも外部に出力することを特徴とするアプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量増大方法。
【請求項８】　ＩＣカードや携帯端末等のようなアプリケーション又はデータ格納メモリを具えた装置であって、少なくとも１つのアプリケーション又はデータが格納されたメモリの使用可能記憶容量を増やすために、前記メモリ内の選択されたアプリケーション又はデータを圧縮し、再使用に解凍する機能、暗号化して外部に出力し、再格納時に復号化する機能、圧縮した後暗号化して外部に出力し、再格納時に復号化した後解凍する機能を有する演算装置と、前記メモリ内に格納されているアプリケーション又はデータの状態が使用可能か、圧縮中か、外部出力中かを示すアプリケーション又はデータ管理表と、を具えたことを特徴とするアプリケーション又はデータ格納メモリを具えた装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はＩＣカードのような耐タンパ装置や携帯端末等のようなアプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量を増やす方法及び装置に関するものである。
【０００２】
【従来技術】近年、金融、通信、交通、公共、医療分野等において、磁気カードに代わる新しい情報記録媒体として、セキュリティ上安全で大きな記憶容量を有するメモリを具えたＩＣカードを用い、これに複数のアプリケ

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－279376
（P2002－279376A）
(43)公開日　平成14年９月27日(2002.9.27)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　19/07		Ｃ０６Ｋ　17/00	Ｄ	２Ｃ００５
Ｇ０６Ｆ　1/00		Ｂ４２Ｄ　15/10	５２１	５Ｂ０３５
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　19/00	Ｎ	５Ｂ０５８
// Ｂ４２Ｄ　15/10	５２１	Ｇ０６Ｆ　9/06	６６０Ｌ	５Ｂ０７６

審査請求　未請求　請求項の数８　ＯＬ　（全　６　頁）

(21)出願番号　特願2001－75632(P2001－75632)

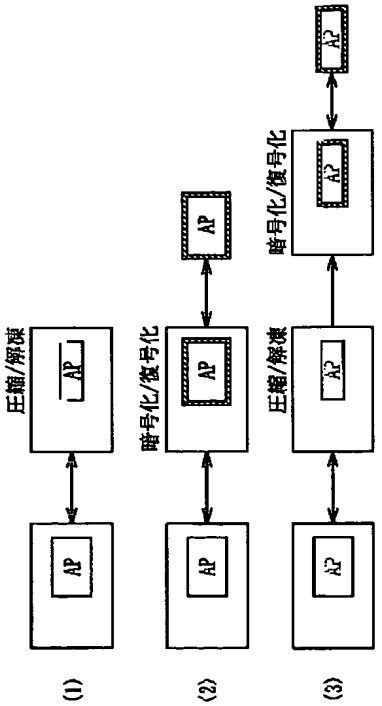
(22)出願日　平成13年３月16日(2001.3.16)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　赤鹿　秀樹
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　平田　真一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100072051
弁理士　杉村　興作　（外１名）

最終頁に続く

(54)【発明の名称】　アプリケーション又はデータ格納メモリを具えた装置の使用可能記憶容量増大方法及び装置

(57)【要約】
【課題】　ＩＣカード又は携帯端末内のアプリケーション又はデータを削除する必要なしに記憶容量を増やす方法を提供することにある。
【解決手段】　アプリケーション格納ＩＣカード又は携帯端末の使用可能記憶容量を増やすために、(1)ＩＣカード又は携帯端末内の暫く不要なアプリケーションＡＰを圧縮する。圧縮したアプリケーションが必要になった際にはこれを解凍し、使用可能にする。(2)ＩＣカード又は携帯端末内にて暫く不要なアプリケーションを圧縮せずに暗号化して外部に出力し、保存する。外部に保存した暗号化されたアプリケーションが必要になった際にはこれをＩＣカード又は携帯端末に戻し、復号化して使用可能にする。(3)ＩＣカード又は携帯端末内にて暫く不要なアプリケーションＡＰを圧縮し、圧縮したアプリケーションを暗号化して外部に出力し、保存する。外部に保存した暗号化された圧縮アプリケーションが必要になった際にはこれをＩＣカード又は携帯端末に戻し、復号化し、解凍して使用可能にする。



METHOD AND DEVICE FOR INCREASING USABLE STORAGE CAPACITY OF DEVICE HAVING APPLICATION OR DATA STORAGE MEMORY

Publication number: JP2002279376
Publication date: 2002-09-27
Inventor: AKASHIKA HIDEKI; HIRATA SHINICHI
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
- international: ***B42D15/10; G06F1/00; G06F21/22; G06K17/00; G06K19/07;*** **B42D15/10; G06F1/00; G06F21/22; G06K17/00; G06K19/07;** (IPC1-7): B42D15/10; G06K19/07; G06F1/00; G06K17/00
- European:
Application number: JP20010075632 20010316
Priority number(s): JP20010075632 20010316

Abstract of **JP2002279376**

PROBLEM TO BE SOLVED: To provide a method for increasing storage capacity, without deleting applications or data in an IC card or a portable terminal. SOLUTION: (1) An application AP which is presently unnecessary in the IC card or the portable terminal is compressed, in order to increase the available storage capacity of the IC card or the portable terminal storing the application. When the compressed application becomes necessary, the application is decompressed to make it useable. (2) An application, presently unnecessary in the IC card or the portable terminal, is not compressed but is coded, and output outside, and then saved. When the application which is saved outside and coded becomes necessary, the application is returned to the IC card or the portable terminal, and decoded to make it usable. (3) The application AP presently unnecessary in the IC card or the portable terminal is compressed, the compressed application is coded and output outside, and then saved. When the compressed application which is saved outside and coded becomes necessary, the application is returned to the IC card or the portable terminal, decoded, and decompressed to make it usable.